UNITED STATES DISTRICT COURT

for the

Central District of California

In the Matter of the Search of A black Samsung cellular phone with a green case and a black Android cellular phone with a black case	)))))	Case No. 2:24-MJ-02668

AMENDED APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Central District of California, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☒ evidence of a crime;

☒ contraband, fruits of crime, or other items illegally possessed;

☒ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession with intent to distribute controlled substances
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 922(g)(1)	Felon in possession of firearm
18 U.S.C. § 924(c)	Carrying a firearm during and in relation to, and possessing a firearm in furtherance of, a drug trafficking crime

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (*give exact ending date if more than 30 days*: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Sean Lusk

Applicant's signature

Sean Lusk, FBI Task Force Officer

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: _____

Judge's signature

City and state: Los Angeles, CA

Honorable Patricia Donahue, U.S. Magistrate Judge

AUSA: Daniel H. Weiner (x 0813)

ATTACHMENT A

PROPERTY TO BE SEARCHED

1. The following digital devices, seized on March 5, 2024:

a. A black Samsung cellular phone with a green case, currently in the custody of the Federal Bureau of Investigation ("FBI") in Los Angeles, California ("SUBJECT DEVICE 1"); and

b. A black Android cellular phone with a black case, currently in the custody of the California Highway Patrol ("CHP") in Santa Maria, California ("SUBJECT DEVICE 2" and collectively the "SUBJECT DEVICES").

ATTACHMENT B

ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 18 U.S.C. § 371 (conspiracy), and 18 U.S.C. §§ 922(g) (prohibited person in possession of a firearm) and 924(c) (carrying a firearm during and in relation to, and possessing a firearm in furtherance of, a drug trafficking crime) (the "Subject Offenses"), namely:

a. Records, documents, programs, applications, materials, or conversations relating to the sale or purchase of controlled substances, including correspondence, receipts, records, and documents noting prices or times when controlled substances were bought, sold, or otherwise distributed;

b. Any photographs of firearms or ammunition, and any paperwork showing the purchase, storage, disposition, or dominion and control over any firearm or ammunition;

c. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of controlled substances;

d. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

e. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the Subject Offenses;

f. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the Subject Offenses;

g. Contents of any calendar or date book;

h. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

i. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense, and forensic copies thereof.

j. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents,

browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

SEARCH PROCEDURE FOR THE SUBJECT DEVICES

4. In searching the SUBJECT DEVICE (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate

the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital devices and/or forensic images thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the

device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICES, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

5. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Sean D. Lusk, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of an application for a warrant to search the following digital devices seized on March 5, 2024 during the arrest of Abraham FAJARDO and Chrystal GASTELUM as described more fully in Attachment A:

a. A black Samsung cellular phone with a green case, currently in the custody of the Federal Bureau of Investigation ("FBI") in Los Angeles, California ("SUBJECT DEVICE 1"); and

b. A black Android cellular phone with a black case, currently in the custody of the California Highway Patrol ("CHP") in Santa Maria, California ("SUBJECT DEVICE 2" and collectively the "SUBJECT DEVICES").

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances), 18 U.S.C. § 371 (conspiracy), and 18 U.S.C. §§ 922(g) (prohibited person in possession of a firearm) and 924(c) (carrying a firearm during and in relation to, and possessing a firearm in furtherance of, a drug trafficking crime) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and

witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only and all dates and times are on or about those indicated.

II. INTRODUCTION

4. I am a Task Force Officer ("TFO") with the FBI assigned to the Central Coast Safe Streets Task Force. I am also employed as a full-time, sworn law enforcement officer for the California Highway Patrol ("CHP") and have been for the past 24 years. I am currently assigned to the Coastal Division Investigative Services Unit. My primary responsibility is to investigate and assist other officers and allied agencies with in-depth investigations involving criminal street gangs, weapons, and narcotics violations.

5. I attended and graduated from the California Highway Patrol Academy and hold Basic, Intermediate, and Advanced Certificates from California Peace Officer Standards and Training. I have completed a 72-hour Drug Recognition Expert course certified by the International Association of Chiefs of Police and over 80 hours of narcotics and criminal interdictions training relating to the transportation, concealment, trends, and sales of illegal narcotics and other criminal activities. I have spoken on numerous occasions with other officers and

experts in the field of narcotics interdiction regarding current trends on narcotic sales and trafficking.

6. As a TFO, I have participated in numerous investigations involving federal firearm and drug offenses and participated in the execution of numerous arrest and search warrants. I have also participated in the interviews of defendants, informants, and witnesses who had personal knowledge of firearm and drug trafficking methods.

III. SUMMARY OF PROBABLE CAUSE

7. On March 5, 2024, two individuals -- later identified as FAJARDO and Chrystal GASTELUM -- led police on a highspeed chase through Santa Barbara County after an attempted traffic stop. After exiting the highway, GASTELUM (the driver) and FAJARDO (the front passenger) drove into a casino parking lot where they exited the car and fled into the casino. Casino surveillance footage shows FAJARDO throwing what appears to be a gun in the trash shortly after exiting the car. During an inventory search of the car after GASTELUM and FAJARDO were arrested, officers found a black bag containing approximately 120 grams of methamphetamine under the driver's seat. FAJARDO has previously been convicted of felony possession of narcotics for sale and being a prohibited person in possession of a firearm. SUBJECT DEVICE 1 was seized from FAJARDO's person following his arrest and SUBJECT DEVICE 2 was seized from the above-described car. Accordingly, I seek this warrant to search the SUBJECT DEVICES for evidence of the Subject Offenses.

IV. STATEMENT OF PROBABLE CAUSE

A. FAJARDO and GASTELUM Flee From a Traffic Stop

8. I know the following based on my review of law enforcement reports, conversations with other law enforcement officers, my review of video and audio recordings of FAJARDO's attempted traffic stop and arrest, review of video surveillance footage, and my own knowledge of the investigation:

a. On March 5, 2024 in Santa Barbara County, at approximately 6:58 a.m., California Highway Patrol ("CHP") Officer Carrier attempted to conduct a traffic stop for speeding on a gray BMW sedan (license plate 8UMM903) traveling northbound on the U.S. 101. Officer Carrier obtained a radar reading of the car traveling at approximately 84 mph. Officer Carrier activated his patrol lights to initiate the stop and the car exited the highway. The car, however, turned back onto the highway (now going southbound) and sped away. Over the next fifteen minutes, the car fled at approximately 130 mph and Officer Carrier eventually lost sight of the car.

b. At around 7:15 a.m., CHP Officer Rodriguez (traveling in a different police car) saw the BMW exit the 101 and turn back onto the highway going northbound. Officer Rodriguez then saw the car turn onto the SR-246 in the direction of the Chumash Casino on the Santa Ynez Indian Reservation, but eventually lost sight of the car. At one point during the chase, Officer Rodriguez saw that a female was driving was the BMW.

c. At around 7:33 a.m., Santa Barbara County Sheriff's Deputy Hollon found the BMW in the parking garage of the Chumash Casino with its engine appearing to still be running. Officers approached the car and determined that it was empty.

B. Law Enforcement Arrest FAJARDO and GASTELUM

9. I know the following based on my review of law enforcement reports, conversations with other law enforcement officers, my review of video and audio recordings of FAJARDO's attempted traffic stop and arrest, review of video surveillance footage, and my own knowledge of the investigation:

a. Law enforcement then worked with Chumash Casino Security Staff to review video surveillance footage to locate the car's passengers. Chumash Casino Staff told law enforcement that footage indicated that a male and female (later identified as FAJARDO and GASTELUM) had already exited the SUBJECT VEHICLE and were walking from the casino's gaming floor to the valet area. Law enforcement then located and detained FAJARDO and a female later identified as the driver of the SUBJECT VEHICLE near the valet parking area outside of Chumash Casino. SUBJECT DEVICE 1 was seized from FAJARDO during his arrest.

C. Law Enforcement Find Methamphetamine in the BMW

10. I know the following based on my review of law enforcement reports, conversations with other law enforcement officers, my review of video and audio recordings of FAJARDO's attempted traffic stop and arrest, review of video surveillance footage, and my own knowledge of the investigation:

a. Following the arrests, officers called a tow truck to remove the car from the casino's private parking lot. Before the car was towed, CHP Officer Asmussen and Officer Jacobs conducted an inventory search and officers found, among other items a glass pipe in the center console, a glass pipe on the right front floorboard, and a black bag under the driver's seat on the left rear floorboard. Inside the bag, Officer Asmussen found: (i) approximately 120 grams of suspected methamphetamine spread across one large bag and two smaller bags. A later detailed search of the bag revealed, (ii) syringes and a glass pipe; (iii) a debit card in the name of "Hua Wang"; and (iv) a handwritten sheet of paper with the name "Jian Hua Hua Wang" and "71 yr old". A DEA lab later confirmed that the methamphetamine in the three baggies had a net weight of 119.6 grams with a purity of 99%, yielding a total amount of approximately 118.4 grams of pure methamphetamine.

b. Officer Jacobs also found another cell phone in the BMW's center console, which GASTELUM later admitted was her phone (i.e., SUBJECT DEVICE 2).[1] During a later search of the car pursuant to a state search warrant, Officers also found a wallet in the driver's side door that contained a small baggie with suspected heroin and seized SUBJECT DEVICE 2.

[1] On March 5, 2024, Judge James F. Rigali, Superior Court for the County of Santa Barbara, California, authorized a search warrant for both phones described in this warrant.

D. Footage Shows FAJARDO Appearing to Throw a Gun in the Trash

11. I know the following based on my review of law enforcement reports, conversations with other law enforcement officers, my review of jail calls, my review of video surveillance footage, and my own knowledge of the investigation:

a. The following day, officers reviewed a recorded jail call between GASTELUM and an unidentified male, where the male says he is waiting for "YG" (which I know to be FAJARDO's moniker based on the context of the call) to call. GASTELUM agrees and states, so he (YG) can "tell you where it's at." In response, GASTELUM also states that he (YG) possibly hid "it" in a restroom. Based on the context of the call and FAJARDO's previous gun convictions, I therefore believed that GASTELUM was referring to a gun that FAJARDO may have discarded in the casino. Accordingly, I went to the casino to search for a gun, but did not find any. However, after further reviewing additional surveillance footage from the casino's garage from May 5, I saw that FAJARDO appeared to throw a gun in a parking lot trash can shortly after exiting the BMW.[2] Below is a screenshot of the footage:

[2] I did not attempt to recover the gun from the casino's dumpster, as it had already been removed from the premises.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

12. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained

where drug traffickers have ready access to them, such as on their cell phones and other digital devices, in vehicles they use, and/or at the places they reside. Drug traffickers also often keep drugs, drug packaging, scales, and cash in places that are readily accessible to them, and under their physical control, such as in their vehicles and/or places they reside.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashes of narcotics in their

vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence, in their vehicles, or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as Blackberry Messenger, WhatsApp, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

VI. TRAINING AND EXPERIENCE ON FIREARM OFFENSES

13. From my training, personal experience, and the collective experiences related to me by other law enforcement

officers who conduct who conduct firearms investigations, I am aware of the following:

a. Persons who possess, purchase, or sell firearms generally maintain records of their firearm transactions as items of value and usually keep them in their residence, or in places that are readily accessible, and under their physical control, such as, in their vehicles or in their digital devices. It has been my experience that prohibited individuals who own firearms illegally will keep the contact information of the individual who is supplying firearms to prohibited individuals or other individuals involved in criminal activities for future purchases or referrals. Such information is also kept on digital devices.

b. Many people also keep mementos of their firearms, including digital photographs or recordings of themselves possessing or using firearms on their digital devices. These photographs and recordings are often shared via social media, text messages, and over text messaging applications.

c. Those who illegally possess firearms often sell their firearms and purchase firearms. Correspondence between persons buying and selling firearms often occurs over phone calls, e-mail, text message, and social media message to and from smartphones, laptops, or other digital devices. This includes sending photos of the firearm between the seller and the buyer, as well as negotiation of price. In my experience, individuals who engage in street sales of firearms frequently use phone calls, e-mail, and text messages to communicate with

each other regarding firearms that the sell or offer for sale. In addition, it is common for individuals engaging in the unlawful sale of firearms to have photographs of firearms they or other individuals working with them possess on their cellular phones and other digital devices as they frequently send these photos to each other to boast of their firearms possession and/or to facilitate sales or transfers of firearms.

d. Individuals engaged in the illegal purchase or sale of firearms and other contraband often use multiple digital devices.

VII. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

19. As used herein, the term "digital device" includes the SUBJECT DEVICE.

20. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are

replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously

develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

21. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

//

VIII. CONCLUSION

19. For all of the reasons described above, there is probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICES described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this ___th day of May, 2024.

_____

HONORABLE PATRICIA DONAHUE
UNITED STATES MAGISTRATE JUDGE